REMARKS/ARGUMENTS

The Office Action has been carefully considered. The issues raised are respectfully submitted to be traversed and addressed below with reference to the relevant headings appearing under the Detailed Action of the Office Action.

""Claim Rejections – 35 USC § 103"

At pages 2 to 8 of the Office Action, the Examiner has maintained his rejections under 35 U.S.C. §103(a), as the Examiner believes that claims 1 to 4, 6 to 15, and 17 to 20 are unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann *et al*, US Patent Number 5,608,800.

The Applicant respectfully submits that the present claim 1 is patentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann *et al*, US Patent Number 5,608,800.

In particular, the present claim 1 describes the following steps for validating an untrusted authentication chip:

- generating a secret random number;
- calculating a signature for the random number using a signature function, in a trusted authentication chip;
- encrypting the random number and the signature by a symmetric encryption function using a first key, in the trusted authentication chip;
- passing the encrypted random number and the signature from the trusted authentication chip to an untrusted authentication chip;
- decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted authentication chip;
- comparing the signature calculated in the untrusted authentication chip with the signature decrypted;
- in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip;
- encrypting the random number by the symmetric encryption function using the second key, in the trusted authentication chip;

- comparing the two random numbers encrypted using the second key, in the trusted authentication chip;
- in the event that the two random numbers encrypted using the second key match, considering the untrusted chip to be valid, and otherwise, the chip is invalid.

Sony describes a method wherein mutual authentication is performed, by the following steps (see abstract):

1. a reader/writer transmits C1 (code) to an IC card such that a random number RA is encrypted using a key KB.
2. the IC card decrypts code C1 into plain text M1 using key KB.
3. the IC card transmits R/W code C2 such that plain text M1 is encrypted using key KA and code C3 such that a random number RB is encrypted using key KA.
4. R/W decrypts codes C2 and C3 into plain text M2 and plain text M3 using KA.
5. R/W determines plain text M2 and random number RA are the same, therefore *authenticates the IC card.*
6. R/W transmits to IC card a code C4 such that plain text M3 is encrypted using key KB.
7. IC card decrypts code C4 into plain text M4 using key KB.
8. When IC card determines plain text M4 and random number RB are the same, the *R/W is authenticated.*

The Examiner will appreciate that the steps described in Sony are clearly different from the steps described in the present claim 1.

In particular Sony does not describe the use of a signature or signature function. Thus, Sony does not describe:

- calculating a signature for the random number using a signature function;
- encrypting the random number *and* the signature with a key;
- passing the encrypted random number *and* signature from the trusted chip to the untrusted chip;
- decrypting the signature and the random number;
- calculating a signature for the decrypted random number using the signature function;
- comparing the two signatures calculated in the trusted and untrusted chips.

Furthermore, Sony does not describe that in the event that the two signatures match, the decrypted random number is encrypted by the symmetric encryption function using the second key and is returned to the trusted authentication chip. Sony does not describe that once the data is returned to the trusted authentication chip, the random number is encrypted by the symmetric function suing the second key, and the two random numbers are compared.

Additionally, on page 3 of the office action, the Examiner has stated that "*Sony discloses that the protocol is performed between one IC card and a reader/writer, which correspond to the untrusted and trusted authentication chips respectively, of claim 1*". The Applicant respectfully submits that this interpretation of Sony is inconsistent with the description in Sony. As shown above, the method described by Sony, requires the authentication of both the IC card and the reader/writer (see italicised font). Thus, Sony is concerned with mutual authentication, that is, the authentication of two untrusted chips.

Hence, Sony clearly describes a different process to that described in claim 1.

With respect to Hoffmann, Hoffmann describes the transmission of a message from a transmitter SE to a receiver EM, where the message is transmitted by (see column 2 lines 37 to 52):

1. generating random data Z at the transmitter;
2. establishing coupling data K
3. generating a symmetric key E from the combination of the random data Z and the coupling data K by one-was enciphering;
4. generating an enciphered signature S/E by symmetrically enciphering a signature S with the key E;
5. forming an enciphered random data Z/T by using a transfer key T and the random number Z; and,
6. formulating the message to be transmitted, the message including useful data D, enciphered signature S/E, coupling data K, and enciphered random data Z/T.

The formed message is then transmitted, and is checked at the receiver end by the following steps (see column 3 line 60 to column 4 line 7):

1. checking the coupling data for plausibility, the message is rejected if check;

2. recovering the random data Z by deciphering the enciphered random data Z/T by the use of the transfer key T;

3. determining the symmetric key E from the calculated random data Z and the coupling data K;

4. recovering the signature S by deciphering the enciphering signature S/E by using E; and,

5. checking the signature S for errors, if errors exist then the message is rejected.

In contrast to claim 1, Hoffmann does not describe encrypting the random number and the signature by a symmetric encryption function using a first key. Hoffmann describes enciphering a signature by a key E, the key E being formed from the random number Z and coupling data K. The random data Z is then enciphered by a separate transfer key K. Thus, in contrast to claim 1, Hoffmann requires two different keys for initially enciphering the random number and the signature.

Additionally, Hoffmann does not describe comparing two signatures in an untrusted chip, and in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using the second key an returning it to the trusted authentication chip. Hoffmann does not describe that once the data is returned to the trusted authentication chip, the random number is encrypted by the symmetric function using the second key, and the two random numbers are compared. Thus, in contrast to claim 1 Hoffmann only describes a one way transaction.

Furthermore, the Applicant respectfully submits that Sony and Hoffmann are concerned with different security systems, that is, Sony is concerned with authenticating IC cards, and a R/W, and Hoffmann is concerned with validating data, thus, there would be no motivation for a person skilled in the art to combine the two references.

In any event, if the two references were combined, the present claim 1 is patentable over the combination. The combination of Sony and Hoffmann does not describe the use of a first key to encrypt a random number and a signature by a symmetric encryption function, comparing two signatures in an untrusted chip, and in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using the second key an returning it to the trusted authentication chip, and further still, once the

data is returned to the trusted authentication chip, encrypting the random number by the symmetric function using the second key, and then comparing the two random numbers.

Hence, the Applicant respectfully submits, that claim 1 provides a different security system to the combination of Sony and Hoffmann. It will be appreciated by the Examiner, that these differences in security systems are not trivial.

Thus, claim 1 is patentable over Sony in view of Hoffmann.

In light of the above, it is respectfully submitted that the claim rejections have been successfully traversed and addressed. Accordingly, it is respectfully submitted that the claims, and the application as a whole with these claims, are allowable, and a favourable reconsideration is therefore earnestly solicited.

Very respectfully,

Applicants:

SIMON ROBERT WALMSLEY

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762